IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Appellants:	Junbiao Zhang
Serial No.:	10/566,393
Filed:	27 January 2006
For:	Controlling Access to a Network Using Redirection
Examiner:	Jing F. Sims
Art Unit:	2437
Conf. No.:	3745

Mail Stop APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia, 22313-1450

APPEAL BRIEF

May it please the Honorable Board:

This is Appellant's Brief on Appeal from the rejection of Claims 1 to 13, 25-34, 36, and 41-57. The Appellant waives an Oral Hearing for this appeal. Enclosed is a single copy of this Brief

CERTIFICATE OF MAILING

I hereby certify that this correspondence (and any document referred to as being attached or enclosed) is being electronically transmitted to Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date indicated below:

_ _____ ___/Kathleen Lyles/_____

Date

Table of Contents

I. REAL PARTY IN INTERST

The real party in interest of Application Serial No.10/566,393 is the Assignee of record:

Thomson Licensing

46, Quai A. Le Gallo

F-92100 Boulogne-Billancourt

FRANCE

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no related appeals and interferences regarding Application Serial No. 10/566,393, known to the undersigned attorney.

III. STATUS OF THE CLAIMS

Claims 1 to 13, 25-34, 36, and 41-57 have been rejected; the rejection of Claims 1 13, 25-34, 36, and 41-57 is appealed.

III. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the Claims listed in Appendix I.

IV. SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 claims a method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client (page 6, line 30, to page 7, line 1);

re-directing, by said AP, said access request to a local server (at page 6, lines 25- 26);

associating unique data with an identifier of said client and storing a mapping of said association in said AP (page 6, line 30 to page 7, line 3);

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client (page 7, lines 4-6);

transmitting an authentication request to said selected authentication server (page 7, lines 7 to 8); and

receiving a response to said authentication request from said selected authentication server (page 7, lines 8-9).

Independent claim 25 claims a system for controlling access to a network comprising:

a client (page 6, line 30);

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client (page 4, lines 4 and 18); and

an authentication server for performing an authentication process in response to a request from the client (page 3, lines 28-29); wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association (page 6, line 30 to page 7, line 3);

the LS transmits the unique data to the client (page 7, lines 4-6);

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation (page 7, lines 11 to 14).

Independent Claim 42 claims a method for controlling network access, said method comprising:

receiving a request for network access (page 6, lines 25 and 26);

redirecting said request via a message (page 6, line 17);

receiving a client identifier and unique data (page 6, lines 25 to 31);

associating said unique data and said client identifier (page 6, line 30 to page 7, line 1);

receiving a re-directed universal resource locator included embedded information (page 7, lines 10-14);

generating a local digital signature using said embedded information and said association between said unique data and said client identifier (page 7, lines 12-14);

comparing said local digital signature with a digital signature received in said embedded information (page 7, lines 17-20);

granting network access if said local digital signature matches said digital signature received in said embedded in information (page 7, lines 20-21); and

deny network access if said local digital signature does not match said digital signature received in said embedded information (page 7, lines 21-22).

Independent Claim 45 claims a system for controlling network access, comprising:

means (130) for receiving a request for network access (page 6, lines 25-26);

means for redirecting (210) said request (205) via a message (220, page 6, lines 15-17);

means for receiving a client identifier and unique data (page 6, lines 30-31);

means for associating said unique data and said client identifier (page 6 line 30 to page 7, line 1);

means for receiving a redirected universal resource locator included embedded information (page 7, lines 15-17);

means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier (page 7, lines 17-20);

means for comparing said local digital signature with a digital signature received in said embedded information (page 7, lines 18-20);

me for granting network access if said local digital signature matches said digital signature received in said embedded information (25, page 7, lines 20-21); and

means for deny network access if said local digital signature does not match said digital signature received in said embedded information (page 7, lines 21-22).

Independent Claim 48 claims a method for controlling network access, said method comprising:

receiving a re-directed request for network access via a message (page 6, line 17);

transmitting a client identifier and unique data (page 6, lines 30-31); and

generating a web page including embedded data (page 7, lines 4-5).

Independent Claim 51 claims a system for controlling network access, comprising:

means for receiving a redirected request for network access via a message (page 6, line 17);

means for transmitting a client identifier and unique data (page 6, line 32); and

means for generating a web page including embedded data (page 7, lines 4-5).

Independent Claim 54 claims a method for controlling network access, said method comprising:

receiving an authentication user input message (page 7, lines 7-8);

transmitting authentication input page requesting authentication information (page 7, lines 8-9);

receiving authentication credentials (page 7, lines 10-11); and

transmitting an authentication message indicating one of success and failure of an authentication process (page 7, lines 11-12).

V. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

a) Whether Claims 48-57 are properly rejectable under 35 USC 102(b) as anticipated by US 5,708,780 to Levergood et al

b) Whether Claims 1-13, 26, 33, 34, 36 and 41 are properly rejectable under 35 USC 103(a) as unpatentable over US 5,708,780 to Levergood et al in view of US 6,732,176 to Stewart et al and WO 02/39237 to Hinton et al

c) Whether Claims 25, 27-32 and 42-47 are properly rejectable under 35 USC 103(a) as unpatentable over US 5,708,780 to Levergood et al in view of US 6,732,176 to Stewart et al

VI. ARGUMENT

a) Whether Claims 48-57 are properly rejectable under 35 USC 102(b) as anticipated by US 5,708,780 to Levergood et al

Independent Claim 48 claims a method for controlling network access which includes transmitting a client identifier and unique data and generating a webpage including embedded data. Nowhere does Levergood et al show or suggest this method. Levergood et al transmits a service request from a client to a server through a network such as the Internet. Nowhere does Levergood et al show or suggest:

"generating a web page including embedded data",

as specifically recited in Claim 48. Levergood et al does not generate a webpage including embedded data. Rather, Levergood et al gives access to a web page, which webpage does not include embedded data. See column 3, lines 56-57. It is therefore clear that Levergood et al does not affect the patentability of Claim 48.

Claims 49 and 50 are dependent from claim 48 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 48.

Similarly, nowhere does Levergood et al show or suggest:

"means for generating a webpage including embedded data",

as specifically recited in Claim 51. It is therefore clear that the patentability of Claim 51 is not affected by Levergood et al.

Claims 52 and 53 are dependent from Claim 51 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 51.

Similarly, nowhere does Levergood et al show or suggest:

"transmitting authentication input page requesting authentication information",

as specifically set forth in Claim 54. Rather, as explained above, Levergood et al does not generate a web page requesting authentication information, but rather gives access to a web page. It is therefore clear that the patentability of claim 54 is not affect it by Levergood et al.

Claim 55 is dependent from Claim 54 and adds further advantageous features. The Appelant submits that Claim 55 is patentable as its parent Claim 54.

Similarly, nowhere does Levergood et al show or suggest:

"means for transmitting authentication input page requesting authentication information",

as specifically recited in Claim 56. As explained above, Levergood et al does not generate a web page, but rather gives access to a web page. It is therefore clear that the patentability of Claim 56 is not affected by Levergood et al.

Claim 57 is dependent from Claim 56 and adds further advantageous features. The Appellant submits that Claim 57 is patentable as its parent Claim 56.

b) Whether Claims 1-13, 26, 33, 34, 36 and 41 are properly rejectable under 35 USC 103(a) as unpatentable over US 5,708,780 to Levergood et al in view of US 6,732,176 to Stewart et al and WO 02/39237 to Hinton et al

Nowhere does Levergood et al show or suggest:

"generating a web page by said local server requesting that said client select an authentication server",

as specifically set forth in Claim 1. The Examiner admits that Levergood et al does not disclose associating unique data with an identifier of said client and storing a mapping of said association in said AP and generating a web page by said local server requesting that said client select an authentication server. The Examiner asserts that Stewart et al can be combined with Levergood et al to obtain the claimed invention. The Appellant can not agree. Stewart et al provides a plurality of access points 120 to a network 130 which uses a plurality of network providers 160 for access to the Internet. Stewart et al is completely opposite to Levergood et al. Levergood et al use the Internet for access to a server, whereas Stewart et al uses a network 130 as a server for access to the Internet. Because the two systems of Levergood et al and Stewart et al are completely opposite, they are incompatible.

Hinton et al shows another entirely different arrangement. In Hinton et al, a user in one domain obtains an authorization token which allows such user to access a second domain without separate authorization. Hinton et al does not request access through an access point. Hinton et al does not generate a web page which requests a client to select an authorization server. Figure 3B of Hinton et al shows a web page, but such webpage does not request:

"that said client select an authentication server",

as specifically recited in Claim 1. Rather, the web page shown in Figure 3 of Hinton et al gives several web site choices, but does not give any choice of authentication server. It is therefore clear that even if the disclosures of Levergood et al, Stewart et al and Hinton et al were to be combined, the patentability of the invention defined by Claim 1 would not be affected.

Claims 2-13, 34, 36 and 41 are dependent from Claim 1 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 1.

Claims 26 and 33 are dependent from Claim 25. These claims are discussed below with regard to Ground c).

c) Whether Claims 25, 27-32 and 42-47 are properly rejectable under 35 USC 103(a) as unpatentable over US 5,708,780 to Levergood et al in view of US 6,732,176 to Stewart et al

The Examiner has asserted that Levergood et al discloses a system for controlling access to a network comprising an access point coupled to a local server for relaying network communications to and from the client. The Appellant can not agree. Levergood et al does not request access to a network. Rather, Levergood et al requests access to a server through a network, such as the Internet. Levergood et al does not request access is to a network through an access point. The Examiner considers the Internet to be an access point. This is contrary to all definitions of an access point. Nevertheless, if the Internet is an access point, Levergood et al has no:

" access point coupled to a local server for relaying network communications to and from the client",

as recited in Claim 25. Furthermore, nowhere does Levergood et al show or suggest:

"the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association",

as recited in Claim 25. Levergood et al does not store a mapping of the association in the Internet. The Appellant has pointed out above why Levergood et al and Stewart et al can not be combined. Stewart et al provides a plurality of access points 120 to a network 130 which uses a plurality of network providers 160 for access to the Internet. Stewart et al is completely opposite to Levergood et al. Levergood et al use the Internet for access to a server, whereas Stewart et

al uses a network 130 as a server for access to the Internet. Because the two systems of Levergood et al and Stewart et al are completely opposite, they are incompatible.

Claims 26-33 are dependent from claim 25 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 25.

With regard to Claim 42, the Examiner has admitted that Levergood et al. does not show associating said unique data and said client identifier. The Examiner looks to Stewart et al for this disclosure. The Appellant can not agree. Stewart et al provides a plurality of access points 120 to a network 130 which uses a plurality of network providers 160 for access to the Internet. Stewart et al is completely opposite to Levergood et al. Levergood et al use the Internet for access to a server, whereas Stewart et al uses a network 130 as a server for access to the Internet. Because the two systems of Levergood et al and Stewart et al are completely opposite, they are incompatible. The Appellant therefore submits that the patentability of Claim 42 is not affected by the combination of Levergood et al. and Stewart et al.

Claims 43 and 44 are dependent from Claim 42 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 42.

Claim 45 is a system claim similar to method Claim 42. Again, the Examiner admits that Levergood et al. does not show "associating said unique data and said client identifier". The Examiner looks to Stewart et al for this disclosure. The Appellant can not agree. Stewart et al provides a plurality of access points 120 to a network 130 which uses a plurality of network providers 160 for access to the Internet. Stewart et al is completely opposite to Levergood et al. Levergood et al use the Internet for access to a server, whereas Stewart et al uses a network 130 as a server for access to the Internet. Because the two systems of Levergood et al and Stewart et al are completely opposite, they are

incompatible. The Appellant therefore submits that the patentability of Claim 45 is not affected by the combination of Levergood et al. and Stewart et al.

Claims 46 and 47 are dependent from Claim 45 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 45.

The Appellant submits that all of the rejected Claims are allowable, and that the Rejection should be reversed.

Respectfully submitted,
JUNBIAO ZHANG

By: ___/Daniel E. Sragow/_____
Daniel E. Sragow, Attorney
Reg. No. 22,856
(609) 734-6832

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

APPENDIX I. APPEALED CLAIMS

1. A method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client;

re-directing, by said AP, said access request to a local server;

associating unique data with an identifier of said client and storing a mapping of said association in said AP;

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

transmitting an authentication request to said selected authentication server; and

receiving a response to said authentication request from said selected authentication server.

2. The method according to claim 1, wherein said network is a wireless Local Area network (WLAN).

3. The method according to claim 1, further comprising:

forwarding said identifier of said client from said local server; and

generating said unique data for said client by said local server.

4. The method according to claim 1, further comprising:

retrieving, by said client, a re-directed URL having embedded data including a first digital signature, authentication parameters and said unique data and forwarding said re-directed URL to said AP;

creating, by said AP, a second digital signature using said authentication parameters, said unique data and said identifier;

comparing, by said AP, said first digital signature with said second digital signature;

determining, by said AP, if there is a match between said first digital signature and said second digital signature; and

performing, by said AP, one of granting network access and denying network access based on said match determination.

5. The method according to claim 1, wherein said unique data includes a session ID and a randomized number.

6. The method according to claim 1, wherein said identifier is an address of said client.

7. The method according to claim 1, wherein the act of authenticating further comprises:

processing, by said AS, said authentication request, wherein said authentication request includes a session ID embedded in said authentication request;

responding to said authentication request by forwarding to said client by said AS an authentication input page, said authentication input page including a request for authentication information; and

receiving, by said AS, authentication credentials from said client, wherein said response to said authentication request forwarded to said client includes a re-direct header and a success code and associated information relevant to access of said network by said client.

8. The method according to claim 7, wherein the act of forwarding further comprises generating, by said AS, said success code and said associated information includes a first digital signature and authentication parameters.

9. The method according to claim 5, wherein said randomized number is one of a random number and a pseudo-random number.

10. The method according to claim 1, wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client.

11. The method according to claim 1, wherein said AP and said local server are co-located.

12. The method according to claim 4, wherein said first and said second digital signatures are generated using one of a private key of said AS and a shared key between said AS and said local server.

13. The method according to claim 4, wherein said second digital signature is locally generated at said AP.

Claims 14-24 (CANCELLED)

25. A system for controlling access to a network comprising:

a client;

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client; and

an authentication server for performing an authentication process in response to a request from the client; wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association;

the LS transmits the unique data to the client;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation.

26. The system of claim 25, wherein the network is a wireless local area network (WLAN) comprising the access point and local server.

27. The system of claim 25, wherein the local server generates a web page requesting that the client select an authentication server, and embeds the unique data in the web page for transmission to the client.

28. The system of claim 25, wherein the identifier of the client is one of a physical address, MAC address and an IP address, and wherein the unique data comprises a session ID and a randomized number.

29. The system of claim 28, wherein the session ID and randomized number are generated by the local server.

30. The system of claim 28, wherein the authentication server receives user credential information from the client and provides a digitally signed authentication message including an authentication parameters using said unique data through HTTPS to the client via said re-direct header to the client.

31. The system of claim 30, wherein the AP, in response to receiving the digitally signed authentication message re-directed from the client including the authentication parameters and at least a portion of the unique data from the client, generates a local digital signature using the received portion of the unique data and the stored mapping data together with the authentication parameters, and compares the local digital signature with the digitally signed authentication message to determine network access by the client.

32. The system of claim 25, wherein the re-direct header further comprises a means for re-directing a browser of the client to a URL on the network, and embedding in the URL said digitally signed authentication message, the authentication parameters and a portion of the unique data.

33. The system of claim 26, wherein said AP and said LS are co-located.

34. The method of Claim 1, further comprising:

at the authentication server, authenticating the client using the unique data, and forwarding said response to the client using a re-direct header, and including a digitally signed authentication message and authentication parameters corresponding to the unique data; and

the access point receiving from the client according to the re-direct header the digitally signed authentication message and authentication parameters and correlating the authentication parameters with the mapped association data for determining access to the network.

Claim 35. (CANCELLED)

36. The method of Claim 1, wherein said unique data comprises a session ID and a randomized number and further comprising: receiving, by said AP, a re-directed request from the client and including a digitally signed authentication message, an authentication parameter list, and said session ID, the digitally signed authentication message being generated using the randomized number, said session ID and said authentication parameter list, by said selected authentication server associated with the client; and

correlating the received digitally signed authentication message with the re-directed request for access using the stored mapping data for controlling access by the client to the network.

Claims 37-40 (CANCELLED)

41. The method according to claim 36, wherein said AP and said LS are co-located.

42. A method for controlling network access, said method comprising:

receiving a request for network access;

re-directing said request via a message;

receiving a client identifier and unique data;

associating said unique data and said client identifier;

receiving a re-directed universal resource locator included embedded information;

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

43. The method according to claim 42, wherein said unique data comprises a session identifier and a random number.

44. The method according to claim 42, wherein said embedded information further comprises a session identifier and authentication parameters.

45. A system for controlling network access, comprising:

means for receiving a request for network access;

means for re-directing said request via a message;

means for receiving a client identifier and unique data;

means for associating said unique data and said client identifier;

means for receiving a re-directed universal resource locator included embedded information;

means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

means for comparing said local digital signature with a digital signature received in said embedded information;

means for granting network access if said local digital signature matches said digital signature received in said embedded information; and

means for deny network access if said local digital signature does not match said digital signature received in said embedded information.

46. The system according to claim 45, wherein said unique data comprises a session identifier and a random number.

47. The system according to claim 45, wherein said embedded information further comprises a session identifier and authentication parameters.

48. A method for controlling network access, said method comprising:

receiving a re-directed request for network access via a message;

transmitting a client identifier and unique data; and

generating a web page including embedded data.

49. The method according to claim 48, wherein said unique data comprises a session identifier and a random number.

50. The method according to claim 48, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

51. A system for controlling network access, comprising:

means for receiving a re-directed request for network access via a message;

means for transmitting a client identifier and unique data; and

means for generating a web page including embedded data.

52. The system according to claim 51, wherein said unique data comprises a session identifier and a random number.

53. The system according to claim 51, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

54. A method for controlling network access, said method comprising:

receiving an authentication user input message;

transmitting authentication input page requesting authentication information;

receiving authentication credentials; and

transmitting an authentication message indicating one of success and failure of an authentication process.

55. The method according to claim 54, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.

56. A system for controlling network access, comprising:

means for receiving an authentication user input message;

means for transmitting authentication input page requesting authentication information;

means for receiving authentication credentials; and

means for transmitting an authentication message indicating one of success and failure of an authentication process.

57. The system according to claim 56, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.

APPENDIX II. EVIDENCE

None

APPENDIX III. RELATED PROCEEDINGS

The Appellant asserts that there are no proceedings related to the instant appeal.